UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,504	06/23/2006	Udo Doebrich	2003P05083WOUS	8240

22116 7590 07/29/2008

SIEMENS CORPORATION
INTELLECTUAL PROPERTY DEPARTMENT
170 WOOD AVENUE SOUTH
ISELIN, NJ 08830

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
07/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	**Applicant(s)**
Office Action Summary	10/563,504	DOEBRICH ET AL.
	Examiner	**Art Unit**
	Christian LaForgia	2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>*3*</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24,25,27-30,33-35,37 and 40-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24,25,27-30,33-35,37 and 40-51* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2006* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 15 July 2008 has been entered.

2. Claims 24, 25, 27-30, 33-35, 37, and 40-51 have been presented for examination.

3. Claims 1-24, 26, 31, 32, 36, 38, and 39 have been cancelled as per Applicant's request.

Response to Arguments

4. Applicant’s arguments, see page 8, filed 19 June 2008, with respect to the claim objections have been fully considered and are persuasive. The objections of claims 30, 37, and 40 have been withdrawn.

5. Applicant's arguments with respect to the prior art rejection of claims 24, 25, 27-30, 33-35, 37, and 40-51 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 24, 25, 27-30, 33-35, 37, 50, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,215,775 B2 to Noguchi et al., hereinafter Noguchi, in view of U.S. Patent No. 6,947,559 B2 to Gleeson, hereinafter Gleeson.

8. As per claim 24, Noguchi teaches a method and communication system for transmitting data, comprising:

by a first user of a communication network:

generating a first symmetrical encryption key based on the first random value (Figures 4, 10 [block 33], column 9, lines 41-50, column 12, lines 13-19);

a storage unit for storing the first symmetrical encryption key (Figure 10 [block 35], column 12, lines 22-25); and

transmitting the first random value to a second user of the communication network (Figures 4, 10 [block 31], column 9, lines 41-44, column 12, lines 17-22, i.e. sending a random number R and an ID that specifies an key generation algorithm to source A from destination B);

by the second user:

receiving the first random value from the first user (Figures 4, 10 [block 31], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc); and

generating the first symmetrical encryption key based on the received random value (Figures 4, 10 [block 33], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc).

9. Noguchi does not teach wherein the random value is generated from a stochastic process, wherein the first rand value comprises a digital value derived from a sensor output of an operational measurement of an automation system.

10. Gleeson teaches measuring a physical property, such as absorbance, transmittance, reflectance, or current flow values which are than turned into a random number which is used to generate a key to encrypt data (column 2, lines 23-38, column 3, lines 4-13).

11. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the random value be generated from a stochastic process, since Gleeson states at column 1, lines 7-20 that generating a random number in this manner are essential for strong data encryption, thereby preventing interlopers from gaining unauthorized access to the encrypted data.

12. Regarding claim 25, Gleeson teaches wherein the first random value is an input to a function and an output of the function is used to generate the first encryption key (column 2, lines 23-38, column 3, lines 4-13).

13. Regarding claim 27, Gleeson teaches wherein the first random value is obtained by acquiring at least one measured value from the first stochastic process (column 2, lines 23-38).

14. Regarding claim 28, Gleeson teaches wherein the first stochastic process includes a time-variable parameter of an automation system (column 3, lines 44-62).

15. Regarding claim 29, Gleeson teaches wherein the first random value is a measured value (column 2, lines 23-38, column 3, lines 4-13).

16. Gleeson and Noguchi do not disclose wherein the first user generates the first symmetrical encryption key based on the least significant bits of the first random value in order to at least reduce periodic components of the measure value; and wherein the second user

generates the first symmetrical encryption key based on the least significant bits of the first random value in order to at least reduce periodic components of the measure value.

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to obtain the data from a least significant bit position of the measured data, since it is a well-known and common practice in art to read data from the least significant bit and merely amounts to a design choice.

18. Regarding claims 30 and 42, Noguchi teaches wherein data transferred between the users is encrypted and unencrypted via the symmetrical encryption keys (Figure 4 [cipher communication using the symmetric keys]).

19. Noguchi and Gleeson do not disclose wherein the second user receives a second random value originating from a second stochastic process; generating a second symmetrical encryption key from a second stochastic process; transmitting the second random value to the first user; and the first user: receiving the second random value from the second user; and generating the second symmetrical encryption key based on the received random value.

20. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the method of claims 24 and 40, respectively, for the second client, since it has been held that it only requires routine skill in the art to duplicate a method and that said duplication has no patentable significance unless new and unexpected results are produced. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

21. With regards to claim 33, Noguchi and Gleeson do not teach wherein the first and second symmetrical encryption keys are generated upon a request by a master user of the communication network.

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

23. With regards to claim 34, Gleeson teaches wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval (column 3, lines 44-62).

24. Regarding claim 35, Noguchi and Gleeson do not teach wherein the first random value are transmitted over the communication network at a time of low utilization of the communication network.

25. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit data over the network at a time of low utilization, since one of ordinary skill in the art would realize that retrieving information about the communication channel when utilization was low would provide for better results without interference from any cross communication occurring on the network.

26. Regarding claim 37, Noguchi teaches wherein the first random value is transmitted using an asymmetrical encryption method (column 9, lines 20-50, i.e. destination B encrypts the random number R using the public key Kp received from source A).

27. Regarding claim 50, Gleeson teaches wherein the first random value comprises a combination of at least two digital values obtained from respective different sensors indicating respective different operational measurements of an automation system (column 3, line 47-62, coupling and mixing values).

28. With regards to claim 51, Gleeson teaches wherein the first random value comprises a concatenation of at least two digital values obtained from respective different sensors indicating respective different operational measurements of an automation system (column 3, line 47-62, coupling and mixing values).

29. Claims 40-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Gleeson, and further in view of U.S. Patent Application Publication No. 2002/0154769 A1 to Petersen et al., hereinafter Petersen.

30. Claim 40 is rejected on the same grounds as claim 24 above, although Noguchi and Gleeson do not teach removing at least one high order bit from the digital value to reduce a periodic component of the operation measurement.

31. Petersen teaches deleting the most significant bits from the digital value so that the value would fit in a designated register (paragraph 0039).

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to remove at least one high order bit from the digital value to reduce a periodic component of the operation measurement, since Petersen shows that removing high order bits is something well-known and commonly practiced. Something old does not become patentably distinct upon the discovery of a new property, such as reducing the periodic component of a measured value in the present case. The claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable. See *In re Best*, 562 F.2d 1252, 1254, 195 USPQ 430, 433 (CCPA 1977); see also MPEP 2112(I).

33. Regarding claim 41, Noguchi teaches wherein the communication network is a public network (Figure 13 [elements 84, 92], column 13, lines 48-63).

34. With regards to claim 43, Noguchi teaches wherein the communication network is the Internet (Figure 13 [elements 84, 92], column 13, lines 48-63).

35. Noguchi, Gleeson and Petersen do not teach that the first user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the Internet.

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted

communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

37. With regards to claim 44, Noguchi, Gleeson, and Petersen do not teach wherein the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since the references do not disclose a third-party for initiating encrypted communications between the two parties.

39. Regarding claim 45, Noguchi, Gleeson, and Petersen do not teach wherein the first random value is transmitted to a plurality of users and the first symmetrical encryption key is generated at each of the plurality of users.

40. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the first user transmit the random value to a plurality of users, especially so since Noguchi includes identifying which algorithm to use to generate the key, since one of ordinary skill in the art would recognize the need for providing secure communications in a group type setting.

41. Claim 46 is rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Gleeson in view of Petersen as applied above, and further in view of U.S. Patent No. 6,973,499 B1 to Peden et al., hereinafter Peden.

42. With regards to claim 46, Noguchi, Gleeson, and Petersen do not teach wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

43. Peden teaches wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval (column 6, lines 10-24, claim 18, i.e. a plurality of keys, wherein each key corresponds to one of a plurality of time intervals and each key being a symmetric key).

44. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first symmetrical encryption key to be used to encrypt data transmitted during a first time interval and the second symmetrical encryption value to be used to encrypt data transmitted during a second time interval, since Peden states at column 2, lines 14-31 that designating keys for certain time periods prevents unauthorized users from accessing data in an environment that has a constantly changing base of users.

45. Claims 47-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noguchi in view of Gleeson in view of Petersen, and further in view of U.S. Patent No. 6,973,499 B1 to Peden et al., hereinafter Peden.

46. As per claim 47, Noguchi teaches a method for transmitting data, comprising

by a first user of a communication network:

storing a first random measured value (Figure 10 [block 35], column 12, lines 22-25);

generating a first symmetrical encryption key based on the first random measured value (Figures 4, 10 [block 33], column 9, lines 41-50, column 12, lines 13-19);

transmitting the first measured random value to a second user of the communication network (Figures 4, 10 [block 31], column 9, lines 41-44, column 12, lines 17-22, i.e. sending a random number R and an ID that specifies an key generation algorithm to source A from destination B);

by the second user:

receiving the first random measured value from the first user (Figures 4, 10 [block 31], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc);

generating the first symmetrical encryption key based on the received measured random value (Figures 4, 10 [block 33], column 9, lines 51-56, i.e. source A uses random number R to generate symmetric key Kc).

47. Noguchi does not teach wherein the random value is generated from a stochastic process, wherein the first rand value comprises a digital value derived from a sensor output of an operational measurement of an automation system.

48. Gleeson teaches measuring a physical property, such as absorbance, transmittance, reflectance, or current flow values which are than turned into a random number which is used to generate a key to encrypt data (column 2, lines 23-38, column 3, lines 4-13).

49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the random value be generated from a stochastic process, since Gleeson states at column 1, lines 7-20 that generating a random number in this manner are essential for strong data encryption, thereby preventing interlopers from gaining unauthorized access to the encrypted data.

50. Noguchi and Gleeson do not disclose wherein the second user receives a second random value originating from a second stochastic process; generating a second symmetrical encryption key from a second stochastic process; transmitting the second random value to the first user; and the first user: receiving the second random value from the second user; and generating the second symmetrical encryption key based on the received random value and wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

51. It would have been obvious to one of ordinary skill in the art at the time the invention was made to duplicate the method generating the first client's symmetric key for the second client, since it has been held that it only requires routine skill in the art to duplicate a method and that said duplication has no patentable significance unless new and unexpected results are produced. See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 124 USPQ 378 (CCPA 1960).

52. Noguchi and Gleeson do not teach removing at least one high order bit from the digital value to reduce a periodic component of the operation measurement.

53. Petersen teaches deleting the most significant bits from the digital value so that the value would fit in a designated register (paragraph 0039).

54. It would have been obvious to one of ordinary skill in the art at the time the invention was made to remove at least one high order bit from the digital value to reduce a periodic component of the operation measurement, since Petersen shows that removing high order bits is something well-known and commonly practiced. Something old does not become patentably distinct upon the discovery of a new property, such as reducing the periodic component of a measured value in the present case. The claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable. See *In re Best*, 562 F.2d 1252, 1254, 195 USPQ 430, 433 (CCPA 1977); see also MPEP 2112(I).

55. Peden teaches wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval (column 6, lines 10-24, claim 18, i.e. a plurality of keys, wherein each key corresponds to one of a plurality of time intervals and each key being a symmetric key).

56. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first symmetrical encryption key to be used to encrypt data transmitted during a first time interval and the second symmetrical encryption value to be used to encrypt data transmitted during a second time interval, since Peden states at column 2, lines 14-31 that designating keys for certain time periods prevents unauthorized users from accessing data in an environment that has a constantly changing base of users.

57. Regarding claim 48, Gleeson teaches wherein the first random value is an input to a function and an output of the function is used to generate the first symmetrical encryption key (column 2, lines 23-38, column 3, lines 4-13).

58. Regarding claim 49, Gleeson teaches wherein the second random value is an input to a function and an output of the function is used to generate the second symmetrical encryption key (column 2, lines 23-38, column 3, lines 4-13).

Conclusion

59. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

60. The following patents are cited to further show the state of the art with respect to generating keys from randomly measured values, such as:

United States Patent Application Publication No. 2002/0131592 A1 to Hinnant, which is cited to show measuring inertial values to use as a seed to generate an encryption key.

United States Patent No. 5,781,458 to Gilley, which is cited to show creating truly random numbers for cryptographic key generation.

61. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

62. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

63. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

Clf